32860-000704/US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

INFORMATION SHEET

Applicant(s): Thomas BIRKHOELZER; Frank KRICKHAHN; and Juergen VAUPEL

Application No: **NEW APPLICATION**

Filed: February 25, 2004

For: METHOD FOR THE ENCRYPTION AND DECRYPTION OF DATA BY VARIOUS USERS

Priority Claimed Under 35 U.S.C. §119 and/or 120:

COUNTRY	DATE	NUMBER
GERMANY	February 25, 2003	103 07 996.3

Send correspondence to : HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 8910
Reston, VA 20195
(703) 668-8000

The above information is submitted to advise the United States Patent and Trademark Office of all relevant facts in connection with the present application. A timely executed Declaration in accordance with 37 CFR 1.64 will follow.

Respectfully submitted,

By _____
Donald D. Daley
Reg. No. 34,313
P.O. Box 8910
Reston, VA 20195
(703) 668-8000

DJD:jcp

PATENT
32860-000704/US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: **NEW APPLICATION**

Filing Date: February 25, 2004

Applicants: Thomas BIRKHOELZER et al.

Title: METHOD FOR THE ENCRYPTION AND DECRYPTION OF DATA BY VARIOUS USERS

PRIORITY LETTER

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

February 25, 2004

Dear Sirs:

Pursuant to the provisions of 35 U.S.C. 119, enclosed is/are a certified copy of the following priority document(s).

Application No.	Date Filed	Country
103 07 996.3	February 25, 2003	GERMANY

In support of Applicant's priority claim, please enter this document into the file.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____
Donald J. Daley, Reg. No. 34,313

DJD:jcp

P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

Enclosure

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	103 07 996.3
Anmeldetag:	25. Februar 2003
Anmelder/Inhaber:	Siemens Aktiengesellschaft, 80333 München/DE
Bezeichnung:	Verfahren zum Ver- und Entschlüsseln von Daten durch verschiedene Nutzer
IPC:	H 04 L 9/32

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 05. Februar 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Stark

A 9161
06/00
EDV-L

Beschreibung

Verfahren zum Ver- und Entschlüsseln von Daten durch verschiedene Nutzer

Die Erfindung betrifft ein Verfahren zum Ver- und Entschlüsseln von Daten durch verschiedene Nutzer. Die Erfindung betrifft außerdem eine Datenverarbeitungseinrichtung zur Durchführung des Verfahrens sowie ein Speichermedium, auf dem Information, z.B. ein Computer-Programm, zur Ausführung des Verfahrens gespeichert ist.

Die vermehrte Nutzung elektronischer Daten und Kommunikationswege bringt ständig wachsende Anforderungen an den Schutz der Daten vor unerwünschten Datenzugriffen, gleichzeitig aber auch an die möglichst einfache, bequeme und unaufwändige Zugreifbarkeit der Daten mit sich. Insbesondere aufgrund der zunehmenden gegenseitigen Vernetzung und der häufig großen Anzahl verschiedener Nutzer, die physikalischen Zugang zu bestimmten Daten erlangen können, sind wirksame elektronische oder software-basierte Kontroll- und Schutzmechanismen unerlässlich geworden.

Der effektive Schutz von vielfältig zugreifbaren Daten vor unberechtigtem Zugriff spielt eine bedeutende Rolle. Eine Vielzahl von Verschlüsselungs-Mechanismen unter Verwendung symmetrischer oder asymmetrischer Datenschlüssel ist bekannt, von denen die auf Basis asymmetrischer Schlüssel-Systeme arbeitenden Verschlüsselungs-Programme wie PGP zu den sichersten und am bequemsten handhabbaren gehören dürften und daher die weiteste Verbreitung gefunden haben. Sowohl symmetrische als auch asymmetrische Schlüsselsysteme basieren auf der Verwendung zumindest eines individuellen Datenschlüssels, der nur dem berechtigten Nutzer zur Ver- und Entschlüsselung seiner Daten zugänglich sein darf. Der Zugang zu diesem individuellen Schlüssel ist vor nicht berechtigten Nutzern möglichst effektiv zu schützen.

Der Schutz elektronischer Daten vor unberechtigten Zugriffen spielt bei personenbezogenen Daten wie Adresslisten oder Kundendaten, bei Daten im Finanzwesen und insbesondere bei Daten im Gesundheitswesen eine besonders wichtige Rolle. Im Gesundheitswesen, wo strengste Anforderungen an die Datensicherheit gestellt werden, fordern Datenschutzbestimmungen, dass jeder Nutzer von Daten eindeutig identifiziert und authentifiziert wird. Authentifizierung bedeutet, dass die Authentifizierung eines Nutzer in Abhängigkeit von dessen Identifizierung zuerkannt wird und nur authentifizierte Nutzer Zugriff auf die fraglichen Daten erhalten können. Die Funktion der Authentifizierung wird im Gesundheitswesen auch „access control" genannt.

Zusätzlich zur Authentifizierung wird in sicherheitskritischen Datenanwendungen, z.B. in der Telemedizin oder in Home-Care-Systemen, bei jeglicher Kommunikation über grundsätzlich unsichere Kommunikationskanäle und bei jeder Speicherung sicherheitskritischer Daten eine Verschlüsselung gefordert. Bei der Nutzung verschlüsselter Daten kann es vorkommen, dass mehrere unterschiedliche Nutzer die Möglichkeit zum Datenzugriff haben sollen. Dies kann z.B. bei der Verwaltung von Kundendaten durch die Angestellten einer Bank der Fall sein, bei Personaldaten in Personalabteilungen, bei der gemeinsamen Nutzung von Daten in Entwicklungs-Teams oder bei Daten im Gesundheitswesen, die mehreren behandelnden Ärzten oder einem bestimmten Kreis medizinischen Fachpersonals zugänglich sein sollten. Hier besteht das Problem, dass Daten, die von einem bestimmten Nutzer mit seinem individuellen Datenschlüssel verschlüsselt wurden, durch andere Nutzer mit anderen individuellen Datenschlüsseln nicht entschlüsselt werden können.

Um die gemeinsam zu nutzenden verschlüsselten Daten trotzdem bestimmten Nutzerkreisen zugänglich zu machen, ist es häufig üblich, den hierfür erforderlichen Datenschlüssel allen Nutzern mitzuteilen. Die Verteilung des Schlüssels an den Nut-

zerkreis führt zu erheblichen Problemen für die Datensicherheit, da der Schlüssel einer Vielzahl von beteiligten Personen mitgeteilt werden muss, und da es aufgrund der schlechten Memorierbarkeit von sicherheitstechnisch wirksamen Datenschlüsseln nicht unüblich ist, dass diese auf ungeeignete Weise aufbewahrt werden, z.B. auf Notizzetteln in Schreibtischschubladen. Die zentrale Verwaltung der Schlüssel macht außerdem das Führen von Schlüsselbüchern, sogenannten Code-Büchern, erforderlich, deren Ausspionierbarkeit einen weiteren Unsicherheitsfaktor darstellt.

Die Aufgabe der Erfindung besteht darin, die sichere Handhabung von Datenschlüsseln für mehrere, unterschiedliche Nutzer zur Nutzung gemeinsamer verschlüsselter Daten zu vereinfachen.

Die Erfindung löst diese Aufgabe durch ein Verfahren gemäß dem ersten Patentanspruch, durch eine Vorrichtung mit den Merkmalen des achten Patentanspruchs und durch ein Speichermedium mit Information, z.B. einem Computer-Programm, zur Ausführung des Verfahrens gemäß dem vierzehnten Patentanspruch.

Die Erfindung beruht auf der Erkenntnis, dass die Fähigkeit zur Ver- und Entschlüsselung gemeinsam genutzter Daten nicht personenbezogen, sondern gruppenbezogen ist. Jeder Nutzer der gemeinsam zu nutzenden verschlüsselten Daten wird damit nicht mehr als Person, sondern entsprechend seiner Zugehörigkeit zu einer Gruppe identifiziert.

Ein Grundgedanke der Erfindung besteht darin, Personen, die verschlüsselte Daten gemeinsam nutzen, keinen nutzerindividuellen Datenschlüssel zum Zugriff auf die Daten zuzuteilen. Stattdessen wird solchen Personen in Abhängigkeit von ihrer Zugehörigkeit zu einer Nutzer-Gruppe ein gemeinsamer Nutzer-Gruppen-Datenschlüssel zugeteilt. Alle Mitglieder der Nutzer-Gruppe können unter Verwendung des Nutzer-Gruppen-

Datenschlüssel gemeinsam zu nutzende Daten ver- sowie entschlüsseln. Der Datenschlüssel wird automatisch zugeteilt, den Nutzern aber nicht mitgeteilt, d.h. die Nutzer erhalten keine Kenntnis von der tatsächlichen Beschaffenheit des Datenschlüssels. Demzufolge müssen sie sich den Datenschlüssel weder merken, noch können sie ihn kommunizieren. Dadurch werden wesentliche Unsicherheitsfaktoren herkömmlicher Schlüssel-Systeme unterbunden.

Außerdem ergibt sich dadurch der weitere Vorteil, dass bei Änderungen der personellen Zusammensetzung einer Nutzer-Gruppe keine Änderungen des Datenschlüssels erforderlich sind. Insbesondere ist es nicht notwendig, einen neuen Datenschlüssel einzuführen, wenn einzelne Personen die Nutzer-Gruppe verlassen, da diese Personen keine Kenntnis von der Beschaffenheit des Datenschlüssels haben, die sie nach Ausscheiden aus der Gruppe in irgendeiner Weise missbrauchen könnten. Stattdessen erhalten sie beim Versuch, auf Daten zuzugreifen, einfach keinen gültigen Datenschlüssel mehr zugeteilt.

Die Verwendung eines automatisch zugeteilten Nutzer-Gruppen-Datenschlüssels ermöglicht es außerdem, den Datenschlüssel beliebig komplex zu gestalten und beliebig häufig zu wechseln. Es obliegt dem Verschlüsselungs-System, die verschlüsselten Daten-Bestände automatisch umzuschlüsseln, d.h. unter Verwendung des alten Datenschlüssels zu entschlüsseln, unter Verwendung des neuen Datenschlüssels wieder zu verschlüsseln, und den Nutzern zeitlich auf die Umschlüsselung abgestimmt den neuen Nutzer-Gruppen-Datenschlüssel zuzuteilen. Dadurch entfällt jeder Aufwand beim Kommunizieren des neuen Datenschlüssels und beim Abstimmen des Zeitpunkts von dessen Einführung, wodurch weitere Gefahren für die Sicherheit des Verschlüsselungs-Systems unterbunden werden.

Vorteilhafte Ausgestaltungen der Erfindung sind Gegenstand der abhängigen Patentansprüche.

Nachfolgend werden Ausführungsbeispiele der Erfindung anhand von Figuren näher erläutert. Es zeigen:

FIG 1 Flussdiagramm mit den zur Ausführung der Erfindung erforderlichen Verfahrensschritten,

FIG 2 zur Ausführung der Erfindung geeignete Systemarchitektur.

Figur 1 zeigt die Verfahrensschritte, die zur Ausführung der Erfindung erforderlich sind. Das Verfahren startet in Schritt **1** damit, dass ein Datenzugriff erfolgen soll, der den Einsatz eines Kryptografie-Programms zur Ver- oder Entschlüsselung von Daten erforderlich macht. In Schritt **3** wird das Kryptografie-Programm gestartet. Je nach Anwendung kann der Start des Kryptografie-Programms vom Nutzer selbst oder aus einem Anwendungs-Programm heraus automatisch gestartet werden.

In Schritt **5** erfolgt eine Sicherheitsabfrage, mittels derer der Nutzer als real existierende Person identifiziert werden soll. Dazu werden vom Nutzer personen-individuelle Daten erfragt, die allen Anforderungen an die Datensicherheit genügen müssen. Vorzugsweise erfolgt die Sicherheitsabfrage durch eine biometrische Erfassung von charakteristischen und möglichst täuschungssicheren Daten wie Fingerabdruck oder Gestalt der Iris. Daneben besteht die Möglichkeit, dass sich der Nutzer durch eine elektronische Chipkarte oder durch einen elektronischen oder mechanischen Schlüssel ausweisen kann.

In Schritt **7** greift das Kryptografie-Programm auf eine Nutzer-Datenbank zu. In der Nutzer-Datenbank sind Informationen abgelegt, mittels derer der Nutzer unter Verwendung der Daten, die vorher in der Sicherheitsabfrage in Schritt **5** ermittelt wurden, identifiziert werden kann.

In Schritt **9** ermittelt das Kryptografie-Programm auf Basis der Daten aus der Sicherheitsabfrage und der Daten aus der Abfrage der Nutzer-Datenbank die Identität des Nutzers. Der Grad der Täuschungssicherheit bei der Ermittlung der Nutzer-Identität hängt dabei im wesentlichen von der Täuschungssicherheit der Sicherheitsabfrage in Schritt **5** sowie der Datensicherheit der Nutzer-Datenbank ab.

In Schritt **11** fragt das Kryptografie-Programm eine Nutzer-Gruppen-Datenbank ab. Diese enthält Daten, die es erlauben, den Nutzer anhand seiner vorangehend ermittelten Nutzer-Identität einer Nutzer-Gruppe zuzuordnen. Die Nutzer-Gruppen-Datenbank enthält also Informationen über Gruppen von gleichberechtigten Nutzern. Solche Gruppen können z.B. Praxis-Teams aus medizinischem Fachpersonal sein, Mitglieder von Finanzinstituten, Mitarbeiter von Personalabteilungen oder Forschungs-Teams. Allen diesen Gruppen ist gemein, dass sie mit den selben personen- oder objektspezifischen, sicherheitskritischen Daten arbeiten, die zwar allen Team-Mitgliedern zugänglich sein müssen, die jedoch keinesfalls anderweitig zugreifbar sein dürfen.

Die Gruppen-Zugehörigkeit kann sich entweder objektbezogen ergeben, d.h. aus dem Bedürfnis bestimmter Nutzer, mit einem bestimmten Datenbestand arbeiten zu können, oder subjektbezogen, d.h. aus der hierarchischen Berechtigung bzw. Vertraulichkeits-Einstufung des jeweiligen Nutzer, auf Daten eines bestimmten Sicherheits-Levels aufgrund der Stellung im Betrieb grundsätzlich zugreifen zu dürfen. Außerdem kann ein Nutzer mehreren Nutzer-Gruppen angehören, die z.B. mehrere Praxis-Teams repräsentieren, in denen der Nutzer gleichzeitig mitarbeitet. In solchen Fällen hat der Nutzer automatisch Zugriff auf verschiedene, unterschiedliche Datenbestände.

In Schritt **15** fragt das Kryptografie-Programm eine Datenschlüssel-Datenbank ab. Die Datenschlüssel-Datenbank enthält

Informationen, die die Zuteilung bestimmter Datenschlüssel zu bestimmten Nutzern oder Nutzer-Gruppen ermöglichen.

In Schritt **17** ermittelt das Kryptografie-Programm aus der zuvor ermittelten Nutzer-Gruppe und den Daten der Datenschlüssel-Datenbank den oder die zuzuteilenden Datenschlüssel.

In Schritt **19** teilt das Kryptografie-Programm dem jeweiligen Nutzer seinen oder seine Datenschlüssel zu. Dieser Vorgang verläuft für den Nutzer uneinsehbar, da das Kryptografie-Programm den oder die ermittelten Datenschlüssel unmittelbar zur Ver- oder Entschlüsselung von Anwendungs-Daten verwendet. Insbesondere erhält der Nutzer keine Information über die Beschaffenheit der zugeteilten Datenschlüssel. Die Zuteilung eines oder mehrerer Datenschlüssel erfolgt also im Ergebnis der Sicherheitsabfrage automatisch und für den Nutzer unbemerkt.

In Schritt **21** führt das Kryptografie-Programm die angeforderte kryptografische Operation durch, es ver- oder entschlüsselt also Daten zur Benutzung durch den Nutzer oder durch ein anderes, vom Nutzer gestartetes Anwendungsprogramm. In Schritt **23** ist der komplette Kryptografie-Vorgang beendet und der Nutzer wird wieder vom Verschlüsselungs-System abgemeldet.

Das Verfahren zur Ausführung der Erfindung wurde auf Basis der Verwendung von drei unterschiedlichen Datenbanken beschrieben, einer Nutzer-Datenbank, einer Nutzer-Gruppen-Datenbank und einer Datenschlüssel-Datenbank. Die drei Datenbanken repräsentieren die logischen Zuordnungen von Informationen, die im Ablauf des Verschlüsselungs-Verfahrens getätigt werden müssen. Zum ersten muss der Nutzer im Ergebnis der Sicherheitsabfrage identifiziert werden, zum zweiten muss der identifizierte Nutzer einer Nutzer-Gruppe zugeordnet werden und zum dritten muss der zu dieser Nutzer-Gruppe gehörige Datenschlüssel ermittelt werden.

Die Verwendung dreier Datenbanken verleiht dem Verschlüsselungs-System einen modularen Aufbau mit größtmöglicher Flexibilität. In jeder der drei Datenbanken können jederzeit unabhängig von den anderen beiden Datenbanken Änderungen vorgenommen werden. In der Nutzer-Datenbank können die zur Identifikation des Nutzers verwendeten, sicherheitskritischen Informationen regelmäßig geändert werden. In der Nutzer-Gruppen-Datenbank können Änderungen der Gruppen, also der zur gemeinsamen Nutzung von Datenbeständen vorgesehenen Personen, vorgenommen werden, die tatsächliche Änderungen der Zugehörigkeit einzelner Personen zu Nutzer-Teams wiederspiegeln. In der Datenschlüssel-Datenbank können regelmäßig Änderungen der Datenschlüssel vorgenommen werden, um die Sicherheit des Systems zu erhöhen. Damit verbunden ist jeweils das Umschlüsseln des Datenbestandes erforderlich, d.h. das Entschlüsseln mit dem alten und Verschlüsseln mit dem neu einzuführenden Datenschlüssel.

Obwohl der modulare Aufbau mit drei Datenbanken die tatsächlichen logischen Zuordnungen korrekt repräsentiert, ist es selbstverständlich möglich, stattdessen lediglich zwei oder auch nur ein Datenbanksystem zu verwenden.

In **Figur 2** ist eine elektronische Datenverarbeitungseinrichtung **31** dargestellt, auf der das Verfahren zur Ausführung der Erfindung ausgeführt werden kann. Die Datenverarbeitungseinrichtung **31** weist eine Tastatur **33** oder ein sonstiges Eingabegerät sowie einen Bildschirm **35** auf. Je nach Art der Anwendung können auch akustische Ein- und Ausgangssignale verarbeitet werden. Art und Umfang der Ein- und Ausgabegeräte sind für die Ausführung der Erfindung nicht von Belang. Sie hat Zugriff auf einen Anwendungs-Datenspeicher **37**, der der Speicherung vorzugsweise verschlüsselter Anwendungs-Daten dient. Bei der elektronischen Datenverarbeitungseinrichtung kann es sich sowohl um einen medizinischen Arbeitsplatz, z.B. eine

sogenannte Modalität, als auch um einen beliebigen anderen Bildschirmarbeitsplatz, z.B. ein Bankterminal, handeln.

Die Datenverarbeitungseinrichtung **31** ist mit einem Sicherheitsabfrage-Mittel **39** verbunden, das der Ermittlung von Daten zur Identifikation des jeweiligen Nutzers dient. Das Sicherheitsabfrage-Mittel **39** kann in einem Chipkartenleser bestehen, der eine Nutzer-individuelle Chipkarte ausliest. Es kann auch ein mechanisches oder elektronisches Schloss sein, das einen Nutzer-individuellen Schlüssel erfordert. Nicht zuletzt kann es ein Sensor zur Ermittlung biometrischer Daten des Nutzers sein, die beispielsweise die Gestalt von dessen Iris, dessen Fingerabdrücke oder dessen Sprach-Frequenzspektrum misst. Die Verwendung biometrischer Daten im Rahmen der Sicherheitsabfrage weist den Vorteil auf, dass keinerlei Schlüssel oder Karte verwendet werden muss, die der Nutzer verlieren oder die ihm entwendet werden könnten. Darüber hinaus ist die Täuschungssicherheit biometrischer Daten höher einzuschätzen als die von sonstigen Schlüsselsystemen.

Die Datenverarbeitungseinrichtung **31** hat weiter Zugriff auf einen Nutzer-Datenspeicher **41**, der Informationen zur Identifikation von Nutzern anhand der durch die Sicherheitsabfrage-Mittel **39** ermittelten Daten enthält. Diese Daten ermöglichen es dem System, den jeweiligen Nutzer als real existierende Person zu identifizieren.

Die Datenverarbeitungseinrichtung **31** hat außerdem Zugriff auf einen Nutzer-Gruppen-Datenspeicher **43**, der Daten enthält, anhand derer Zuordnungen zwischen Nutzern und Nutzer-Gruppen festgestellt werden können. Durch Abfrage dieser Daten kann das System feststellen, zu welcher Nutzer-Gruppe oder zu welchen Nutzer-Gruppen ein zuvor identifizierter Nutzer gehört.

Die Datenverarbeitungseinrichtung **31** hat außerdem Zugriff auf einen Datenschlüssel-Datenspeicher **45**, der Daten enthält, anhand derer Zuteilungen von Datenschlüsseln zu Nutzern und

Nutzer-Gruppen aufgefunden werden können. Der Datenschlüssel-Datenspeicher enthält offensichtlich die sicherheitskritischsten Informationen des Systems insofern, als er alle Datenschlüssel enthält, anhand derer Daten im Anwendungs-Datenspeicher **37** entschlüsselt werden können.

Für den Datenschlüssel-Datenspeicher **45** gelten besondere Sicherheitsanforderungen, die eine entfernt angeordnete, zentrale Aufstellung dieses Datenspeichers sinnvoll machen können. Zu diesem Zweck greift die Datenverarbeitungseinrichtung **31** auf den Datenschlüssel-Datenspeicher **45** über ein Datenfernverbindungs-Mittel **47** zu. Die entfernte Anbringung des Datenschlüssel-Datenspeichers **45** ermöglicht zum einen deren Trennung von der Datenverarbeitungseinrichtung **31** und dadurch die Trennung von möglichen weiteren Datenverarbeitungseinrichtungen, die mit der Datenverarbeitungseinrichtung **31** vernetzt sein können. Zum anderen ermöglicht sie die Einrichtung besonders strenger Sicherheitsvorkehrungen speziell für den Datenschlüssel-Datenspeicher **45**, wie z.B. besonders restriktive Fire-Walls.

Je nach Sicherheitsvorkehrungen kann das Datenfernverbindungs-Mittel **47** über einen geschützten oder einen ungeschützten Kommunikationskanal verfügen. Außerdem kann der Kommunikationskanal des Datenfernverbindungs-Mittels **47** komplett gesperrt sein und nur in Abhängigkeit vom Ergebnis der Sicherheitsabfrage durch das Sicherheitsabfrage-Mittel **39** geöffnet werden; hierzu kann beispielsweise eine telefonische Modemverbindung verwendet werden.

Je nach Organisation der mit der Datenverarbeitungseinrichtung auszuführenden Arbeiten können die verschiedenen Datenspeicher **37, 41, 43, 45** sämtlich getrennt oder teilweise oder vollständig zusammengefasst sein. Unter Verzicht auf den modularen Aufbau mit einzelnen Datenspeichern und auf die entfernte Anordnung des Datenschlüssel-Datenspeichers **45** können beispielsweise sämtliche relevanten Daten in einem einzigen

lokalen Speicher der Datenverarbeitungseinrichtung **31**, z.B. dessen Festplatte, abgelegt sein. Andererseits kann beispielsweise der Nutzer-Gruppen-Datenspeicher **43** in einer Verwaltungsabteilung aufgestellt sein, die für die Organisation der Arbeitsabläufe und die Zusammenstellung der Nutzer-Gruppen zuständig ist, der Datenschlüssel-Datenspeicher **45** dagegen in einer Informations-Technologieabteilung, die für die Implementierung und Realisierung des Verschlüsselungs-Systems zuständig ist und zuletzt der Nutzer-Datenspeicher **41** in einer für Personen-Daten zuständigen Ausweisstelle, die für die Erfassung und Verifizierung personenspezifischer Erkennungs- oder Sicherheits-Daten zuständig ist.

Wesentlich an der elektronischen Datenverarbeitungseinrichtung zur Ausführung der Erfindung ist lediglich, dass die Sicherheitsabfrage durch das Sicherheitsabfrage-Mittel **39** keinen Rückschluss auf den Datenschlüssel gestattet, den das Verschlüsselungssystem zur Ver- und Entschlüsselung von Anwendungs-Daten verwendet. Diese Trennung bildet die Grundlage dafür, dass ein Datenschlüssel zur Ver- und Entschlüsselung von Daten zuteilt werden kann, der sich dem direkten Zugriff des Nutzers entzieht und für diesen nicht einsehbar ist. Stattdessen erhält der Nutzer durch einen einzigen Anmeldevorgang am System automatisch den oder die für seine Gruppen-Zugehörigkeit definierten Datenschlüssel zum Zugriff auf die verschlüsselten Daten.

Patentansprüche

1. Verfahren zum Ver- und Entschlüsseln von Daten durch verschiedene Nutzer, bei dem einem Nutzer ein Datenschlüssel zur Ver- und Entschlüsselung von Daten zugeteilt wird, wobei in einem ersten Schritt (3) eine Sicherheitsabfrage zur Ermittlung der Identität des Nutzers durchgeführt wird, wobei in einem zweiten Schritt (19) in Abhängigkeit vom Ergebnis der Sicherheitsabfrage ein für den Nutzer nicht einsehbarer Datenschlüssel zuteilbar ist, und wobei verschiedenen Nutzern derselbe Datenschlüssel zuteilbar ist.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass in der Sicherheitsabfrage biometrische Daten des Nutzers abfragbar sind.

3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass in der Sicherheitsabfrage ein Nutzer-individueller elektronischer und/oder mechanischer Schlüssel abfragbar ist.

4. Verfahren nach Anspruch 2 oder 3, dadurch gekennzeichnet, dass der zuzuteilende Datenschlüssel durch Vergleich der in der Sicherheitsabfrage erhaltenen Daten mit dem Inhalt eines Datenschlüssel-Speichers (45) ermittelbar ist.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass der Vergleich der in der Sicherheitsabfrage erhaltenen Daten mit dem Inhalt des Datenschlüssel-Speichers (45) über ein Datenfernverbindungs-Mittel (47) erfolgt.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass einem Nutzer mehrere Datenschlüssel gleichzeitig zuteilbar sind.

7. Verfahren nach einem der vorhergehenden Ansprüche, d a d u r c h g e k e n n z e i c h n e t , dass die Daten medizinisch relevant sind, dass die Nutzer Fachpersonal an einer medizinischen Einrichtung sind, und dass die Nutzer-Gruppen entsprechend den Arbeits-Gruppen innerhalb des Fachpersonals und/oder entsprechend den fachlichen Verantwortlichkeiten gebildet werden.

8. Elektronische Datenverarbeitungseinrichtung (31) zum Ver- und Entschlüsseln von Daten, durch die einem Nutzer ein Datenschlüssel zur Ver- und Entschlüsselung von Daten zuteilbar ist,
d a d u r c h g e k e n n z e i c h n e t , dass die Datenverarbeitungseinrichtung (31) ein Sicherheitsabfrage-Mittel (39) aufweist, durch das eine Sicherheitsabfrage zur Ermittlung der Identität des Nutzers durchführbar ist, dass durch die Datenverarbeitungseinrichtung (31) in Abhängigkeit vom Ergebnis dieser Sicherheitsabfrage ein für den Nutzer nicht einsehbarer Datenschlüssel zuteilbar ist, und dass durch die Datenverarbeitungseinrichtung (31) verschiedenen Nutzern der selbe Datenschlüssel zuteilbar ist.

9. Elektronische Datenverarbeitungseinrichtung (31) nach Anspruch 8,
d a d u r c h g e k e n n z e i c h n e t , dass durch das Sicherheitsabfrage-Mittel (39) biometrische Daten des Nutzers abfragbar sind.

10. Elektronische Datenverarbeitungseinrichtung (31) nach Anspruch 8 oder 9,
d a d u r c h g e k e n n z e i c h n e t , dass durch das Sicherheitsabfrage-Mittel (39) ein Nutzer-individueller elektronischer und/oder mechanischer Schlüssel abfragbar sind.

11. Elektronische Datenverarbeitungseinrichtung (31) nach Anspruch 9 oder 10,

d a d u r c h g e k e n n z e i c h n e t , dass die Datenverarbeitungseinrichtung (31) Zugriff auf einen Datenschlüssel-Speicher (45) hat, um den zuzuteilenden Datenschlüssel durch Vergleich der durch die Sicherheitsabfrage erhaltenen Daten mit dem Inhalt des Datenschlüssel-Speichers (45) zu ermitteln.

12. Elektronische Datenverarbeitungseinrichtung (31) nach Anspruch 11,
d a d u r c h g e k e n n z e i c h n e t , dass der Datenschlüssel-Speicher (45) von der Datenverarbeitungseinrichtung (31) entfernt angeordnet ist, und dass die Datenverarbeitungseinrichtung (31) über ein Datenfernverbindungs-Mittel (47) Zugriff auf den Datenschlüssel-Speicher (45) hat.

13. Elektronische Datenverarbeitungseinrichtung (31) nach Anspruch 8, 9, 10, 11 oder 12,
d a d u r c h g e k e n n z e i c h n e t , dass die Datenverarbeitungseinrichtung (31) ein medizinischer Arbeitsplatz zur Bearbeitung medizinisch relevanter Daten ist.

14. Speichermedium, auf dem Information gespeichert ist, die in Wechselwirkung mit einer Datenverarbeitungseinrichtung (31) treten kann, um das Verfahren nach einem der Ansprüche 1 bis 7 auszuführen.

Zusammenfassung

Verfahren zum Ver- und Entschlüsseln von Daten durch verschiedene Nutzer

Die Erfindung betrifft ein Verfahren zum Ver- und Entschlüsseln von Daten durch verschiedene Nutzer, bei dem einem Nutzer ein Datenschlüssel zur Ver- und Entschlüsselung von Daten zugeteilt wird. Die Erfindung betrifft außerdem eine Datenverarbeitungseinrichtung (31) zur Ausführung des Verfahrens und ein Speichermedium, auf dem Information zur Ausführung des Verfahrens auf einer Datenverarbeitungseinrichtung gespeichert ist. Gemäß der Erfindung wird in einem ersten Schritt (3) eine Sicherheitsabfrage zur Ermittlung der Identität des Nutzers durchgeführt wird. In einem zweiten Schritt (19) wird in Abhängigkeit vom Ergebnis der Sicherheitsabfrage ein für den Nutzer nicht einsehbarer Datenschlüssel zugeteilt. Dabei kann verschiedenen Nutzern, die z.B. einer gemeinsamen Nutzer-Gruppe zuordenbar (13) sind, derselbe Datenschlüssel zugeteilt werden.

FIG 1

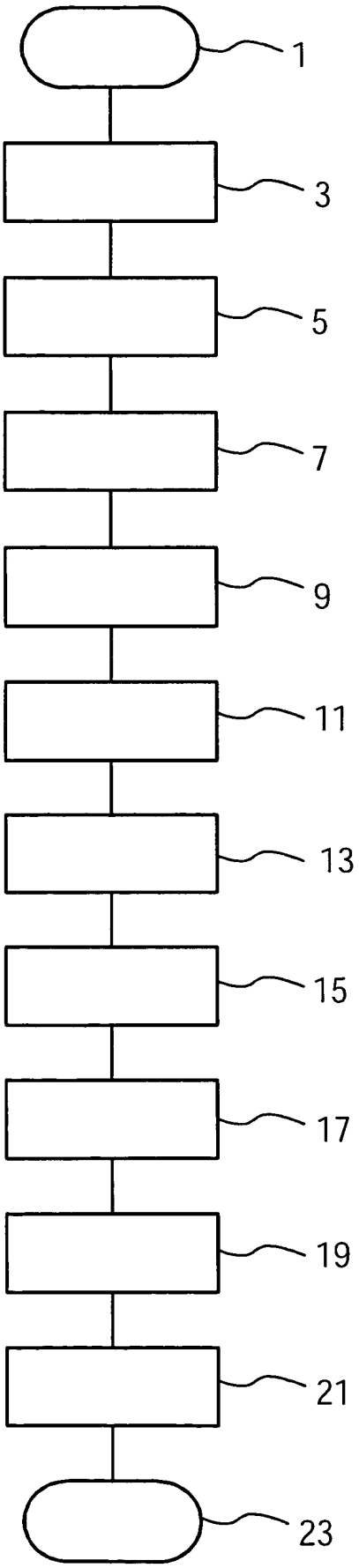

FIG 2